



IT Security Handbook

Risk Assessment

ITS-HBK-2810.04-01 -
Effective Date: 20110506 -
Expiration Date: 20130506 -
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.04-01)
Risk Assessment

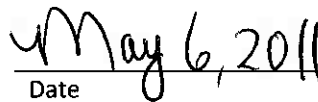
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

| Version | Date | Change Description |
|---------|--------|--------------------|
| 1.0 | 5/2/11 | Initial Draft |
| | | |
| | | |
| | | |
| | | |

Table of Contents

| | |
|--|-----|
| Change History..... | 3 - |
| 1 Introduction and Background..... | 5 |
| 2 Security Categorization (RA-2)..... | 6 |
| 3 Risk Assessment (RA-3)..... | 6 |
| 4 Vulnerability Scanning (RA-5) | 6 |
| 5 Organizationally Defined Values..... | 8 |

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Risk Assessment (RA) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - The Risk Assessment control family relates to a framework for the identification, tracking and mitigation of information security risks. The goal of effective risk management is to articulate the likelihood and impact that threats may have on NASA owned assets, data and personnel, and to minimize the likelihood and impact by applying security controls.
- 1.7 - In order to make informed decisions about the security of NASA assets and personnel, NASA Information System Owners have the responsibility of understanding the risks that affect their system, and the mitigating controls which address them.
- 1.8 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NITR 2800-1, NASA IT Waiver Process*
 - *NPR 1600.1, NASA Security Program Procedural Requirements*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *ITS-HBK-2810.04-02, Risk Assessment: Procedures for Information System Security Penetration Testing and Rules of Engagement*
 - *OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-30, Risk Management Guide for Information Technology Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-39, Managing Risk from Information Systems: An Organizational Perspective*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories*

2 Security Categorization (RA-2)

2.1 Roles and Responsibilities

2.1.1 *The Information System Owner (ISO) shall:*

2.1.1.1 Define system boundaries prior to the system security categorization.

2.1.1.2 Determine the security categorizations of their systems.

2.1.1.2.1 System security categorization shall adhere to the requirements of *FIPS 199*, which distinguishes among systems that have Low, Moderate, or High potential impacts on organizational missions, assets, legal responsibilities, functions, or individuals.

2.1.1.2.2 System security categorizations shall be based on the guidance of *NIST SP 800-37*, *NIST SP 800-60*.

2.1.1.2.3 Information systems that process sensitive data types of a confidential nature (e.g. Sensitive But Unclassified (SBU), Controlled Unclassified Information (CUI)) shall be categorized, at a minimum, as *FIPS 199* Moderate-impact systems for confidentiality.

2.1.1.3 Collaborate with the Information Owner (IO) and Information System Security Officer (ISSO) for proposed system security categorizations.

2.1.2 *The ISSO may:*

2.1.2.1 Provide the ISO with recommendations as to the security categorizations of their systems.

2.1.3 *The IO may:*

2.1.3.1 Provide the ISO with recommendations as to the security categorizations of their systems.

3 Risk Assessment (RA-3)

3.1 Roles and Responsibilities

3.1.1 *The ISO shall:*

3.1.1.1 Ensure the assessment of risk at the system level in a manner consistent with organizationally defined values.

3.1.1.1.1 Risk assessments for NASA information systems and/or information systems that process, store or transmit NASA data shall be conducted in accordance with *NIST SP 800-39*, and *NIST SP 800-30*.

3.1.1.1.2 In accordance with *OMB Memorandum M-04-04*, and related e-authentication initiatives, an e-authentication risk assessment shall be conducted for public users accessing federal information systems.

4 Vulnerability Scanning (RA-5)

4.1 Roles and Responsibilities

4.1.1 *The Senior Agency Information Security Officer (SAISO) shall:*

4.1.1.1 Regularly review and approve the use of Agency tools for vulnerability scanning.

4.1.1.2 Designate patches for critical vulnerabilities of a particularly serious nature that pose a significant threat to the security posture of the Agency as "Expedited".

4.1.2 *The Center Chief Information Security Officer (CISO) shall:*

4.1.2.1 Ensure all NASA information system devices on NASA non-guest networks are subjected to network-based vulnerability scans.

4.1.2.1.1 Scans shall be conducted in a manner consistent with organizationally defined values.

4.1.2.1.2 Scans shall be conducted using a NASA-approved vulnerability scanning tool, and the Agency scan profile, as defined by the Agency Vulnerability Assessment and Remediation (AVAR) project.

4.1.2.2 Ensure the updating of vulnerability signatures on an at-least daily basis.

4.1.2.3 Ensure the capability to automatically update the Information Technology Security Enterprise Data Warehouse (ITSec-EDW) with vulnerability scanning information according to the schedule established by the Agency Security Update Service (ASUS) project.

ITS Handbook (ITS-HBK-2810.04-01) -
Risk Assessment -

- 4.1.2.4 Review and approve ISOs exception from vulnerability scanning when vulnerability scanning threatens to render an information system unusable, or threatens to negatively impact a mission in progress.
 - 4.1.2.4.1 Each approval of exception from vulnerability scanning shall not exceed 30 days.
- 4.1.3 *The Organization Computer Security Official (OCSO) shall:*
 - 4.1.3.1 Execute the vulnerability scanning responsibilities of the Center CISO at the organization level.
- 4.1.4 *The ISO shall:*
 - 4.1.4.1 Ensure the remediation or mitigation of all vulnerabilities as reported by the Agency scan profile in a manner consistent with organizationally defined values.
 - 4.1.4.2 Request temporary exception from vulnerability scanning when vulnerability scanning threatens to render an information system unusable, or threatens to negatively impact a mission in progress.
 - 4.1.4.2.1 Alternative methods to identify vulnerabilities (e.g., adjusting scan settings, researching known vulnerabilities and system configurations which may be at risk) should be investigated and implemented if appropriate.
 - 4.1.4.2.2 Vulnerability scanning shall commence as soon as exceptional circumstances are resolved.
- 4.1.5 *The ASUS Project Manager shall:*
 - 4.1.5.1 Establish a schedule for the automated updating of vulnerability scanning reports in collaboration with the AVAR project.
 - 4.1.5.2 Establish and maintain vulnerability scanning reports in the NASA ITSec-EDW.
 - 4.1.5.3 Ensure the availability of scanning results to the appropriate ISO for analysis and remediation.
- 4.1.6 *The AVAR Project Manager shall:*
 - 4.1.6.1 Determine an Agency-wide vulnerability scanning tool.
 - 4.1.6.2 Assist the ASUS Project Manager with the development of a schedule for the automated updating of vulnerability scanning reports.
 - 4.1.6.3 Ensure the NASA vulnerability management scan profile consists of all current high, non-intrusive vulnerability signatures.
 - 4.1.6.4 Ensure that vendors' highest vulnerability severity ratings are considered "high" in the NASA vulnerability management tool.
 - 4.1.6.5 Provide support and guidance on network vulnerability scanning to all NASA organizations.
 - 4.1.6.6 Maintain Agency hardware, software, and supporting licenses for vulnerability scanning tools.

5

Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

| 800 53 Reference | | | | | | | FIPS 199 Categorization | | |
|------------------|----|---------------------------------------|---------|-----------|-----------|---|--|--|--|
| Family | # | Name | Section | Parameter | Type | Description | Low | Moderate | High |
| RA | 01 | Risk Assessment Policy and Procedures | Main | [1] | Frequency | Policy and procedure review. | 1/Year | 1/Year | 1/Year |
| RA | 03 | Risk Assessment | Main | [1] | Selection | Risk assessment document artifact. | Organization-Defined Document | Organization-Defined Document | Organization-Defined Document |
| RA | 03 | Risk Assessment | Main | [1] [1] | Reference | Organization-Defined Document | Security Assessment Report | Security Assessment Report | Security Assessment Report |
| RA | 03 | Risk Assessment | Main | [2] | Frequency | Review of risk assessments results | 1/Year | 1/Year | 1/Year |
| RA | 03 | Risk Assessment | Main | [3] | Frequency | Update of risk assessment document. | 1/Year | 1/Year | 1/Year |
| RA | 05 | Vulnerability Scanning | Main | [1] | Frequency | Vulnerability scanning. | 1/Month; Credentialed Scanning: 4/Year | 1/Month; Credentialed Scanning: 4/Year | 1/Month; Credentialed Scanning: 4/Year |
| RA | 05 | Vulnerability Scanning | Main | [2] | Reference | Remediation response times. | 30 Days; 7 Days or at the earliest available system maintenance outage, for "Expedited" patches. | 30 Days; 7 Days or at the earliest available system maintenance outage, for "Expedited" patches. | 30 Days; 7 Days or at the earliest available system maintenance outage, for "Expedited" patches. |
| RA | 05 | Vulnerability Scanning | E 2 | [1] | Frequency | Updates to the list of information system vulnerabilities. | 1/Day | 1/Day | 1/Day |
| RA | 05 | Vulnerability Scanning | E 5 | [1] | Reference | Systems for which selected scanning activities requiring privileged access are authorized | | | All Systems |

ITS Handbook (ITS-HBK-2810.04-01) -

Risk Assessment -

| | | | | | | | | | |
|----|----|------------------------|-----|-----|-----------|--|--|--|------------|
| RA | 05 | Vulnerability Scanning | E 7 | [1] | Frequency | Application of automated tools to detect and identify unauthorized software. | | | Continuous |
|----|----|------------------------|-----|-----|-----------|--|--|--|------------|